MOODLEWATCHER: DETECTION AND PREVENTION OF FRAUD WHEN USING MOODLE QUIZZES

Rodolfo Matos, Sofia Torrão, Tito Vieira

University of Porto, Faculty of Engineering (FEUP), Computer Centre (CICA) (PORTUGAL)
rmatos@fe.up.pt, storrao@fe.up.pt, tito@fe.up.pt

Abstract

The possibility of obtaining results that have been fraudulently interfered with always exists, in all processes of student testing and evaluation. In traditional methods of evaluation, such as exams carried out using pen and paper, any fraud that occurs is extremely difficult to detect after it has taken place. The use of e-learning environments such as Moodle, however, may bring benefits that can be applied to the evaluation process in response to this problem. When using Moodle, all actions carried out by participants (regardless of whether they are teachers or students) can be automatically logged by the system, and when carrying out online quizzes this detailed information can be used as an aid in the detection of non-authorized situations that occurred during the process. The aim of this article is to present a tool, developed by the FEUP e-learning team, that permits the auditing and visualization of these situations in quizzes carried out on the Moodle@FEUP platform, thereby permitting the identification of potential offenders in this area. Taking on board the most recent strategies and contexts of testing and evaluation, structural alterations to Moodle are also proposed which will enable the implementation of mechanisms to prevent these new methods of fraud.

1 INTRODUCTION

At the Faculty of Engineering of the University of Porto (FEUP), mechanisms to prevent and improve security in computer-based exams have been in use for quite some time now. Some of these work as a complement to Moodle, and are regularly requested and utilized by the teaching staff. From amongst these mechanisms we can highlight Network Access Restriction (*Restrição de Acesso à Rede*- RAR), which completely blocks all access, whether physical or virtual, to the intranet or Internet. By using the RAR tool with Moodle, teaching staff can set up an exam not only in terms of times and duration but also in order to restrict the taking of the exam to a specific location (e.g. to room B104) and to specify which computers in that location and the time period may be used for the exam. An example of this type of evaluation context would be an exam that has its written component set on Moodle, and which must be answered on Moodle but which permits the use of a determined application for calculations - e.g. the calculator. In this scenario, the teacher needs to create the quiz activity on Moodle, configuring it as if it were an exam (one try only, secure window, and other Moodle configurations), reserving the room for the exam and requesting the security conditions required - Moodle exam with access being allowed only to Moodle and to the calculator. On the date that the exam is to be held, the room(s) is set up for the exam by the CICA team, and the exam takes place in a controlled environment in which all the computers in the allocated rooms only have access to the Moodle server and local access to the authorized applications. Despite these mechanisms, certain situations have recently been detected which demonstrate the creativity shown by students in relation to bending the rules, a spirit which has not been defeated by the introduction of new technologies for evaluation and testing. Access to Moodle, which is permitted for the taking of the exam, also permits access to other Course Units (the *Unidade Curricular* – UC) with areas in Moodle as well as to other activities and resources within the Course Unit to which the exam itself relates. This gives rise to situations in which documents and resources are accessed (such as discussion forums or previous evaluations...) that might be considered to be "unauthorized" elements of consultation, but that students are able to access. As well as the accessing of resources for consultation, students have also been detected exchanging information as well as taking or looking at more than one exam. The Moodle platform does not yet offer a full solution for that problem.

To respond to these situations, and to deal with the challenges that we currently face, it is of utmost importance that we analyze the information conveyed by Moodle logs, an activity that may contribute decisively to the detection of unauthorized or even fraudulent situations. MoodleWatcher is an auditing tool for Moodle logs that facilitates the visualization of these situations.

ISBN: 978-84-615-5563-5

The document that we hereby present is divided into two parts. The first part focuses on giving a more detailed description of the situations of possible fraud that have already been detected and diagnosed, and the second part in which we present the MoodleWatcher tool, with examples of how it may be used to detect this type of circumstance. The document ends by considering the work that still needs to be done, and draws conclusions on work done so far.

2 EXAMPLES OF FRAUD IN MOODLE TESTS

Traditional forms of cheating in exams frequently include "whispering the answer to your neighbour", "crib sheets" and "looking at somebody else's work". We find, on Moodle, methods of cheating that are identical in methodology, but to which we attribute different names:

2.1 Exchange of exams between students

This form of cheating is, according to our records, currently the most popular. The basic method essentially consists of the sharing of the Moodle access code amongst the various participants in the fraud, which allows them to "tell each other the answers" for the exam.

2.2 Use of different accounts from the same workstation

This method consists of accessing one or more different accounts that do not belong to the actual student. This form of fraud is the method used to "take the exam for a friend", and may also be used to see what another student has done.

2.3 Most popular methods of (unauthorized) consultation are:

2.3.1 Looking at blogs

The consultation of blogs is the second most popular method. Students, when accessing their profile, are able to access a method of sharing information that is identical to the archaic system of "pen - paper", but this time using the more modern method of "copy - paste".

2.3.2 Looking at forums

The third most popular method, as with the consultation of blogs, permits the exchange of information between students as well as the simple access of information that has been placed in the system on a previous occasion.

2.3.3 Looking at other resources and suspicious behavior

If even the sharing of information via a Wiki - which amazingly includes the history of all alterations made to the page! – is used by some students to cheat, what can be said for all the other resources that are available on the platform? Needless to say, anyone who spends 30 minutes of a test refreshing the page of a blog belonging to another student is not exactly thinking of taking the test by themselves.

3 THE MOODLEWATCHER TOOL

MoodleWatcher consists of a front-end web application that shares code with Moodle in relation to the use of database access. This integration is, however, limited to the absolute minimum that would enable the tool to be used by the majority of Moodle versions, regardless of their age.

The main purpose of the tool is to provide a simple and efficient monitoring method to be used by teachers in order to assure them of the integrity of the tests and exams carried out using Moodle.

Not all actions carried out on Moodle have a local existence (such as a paper that can be destroyed). The activities of all Moodle users are registered for posterity in a series of actions that can be identified in relation to place and time. The problem up to now was to be found in the actual analysis of these logs, given their size and complexity. MoodleWatcher brings something new to this situation, as it is a method of collating logs in such a way as to permit clear and unequivocal identification - when conformity tests have been carried out - of how and by whom a case of fraud was committed.

When the use of MoodleWatcher is required, a set of conformity tests must be carried out, without which the reliability of the system cannot be guaranteed:

- A test on Moodle does not permit more than one attempt to be made;
- The time of starting and finishing are already defined;
- IP restriction (subnet) is set by the RAR system.

Besides these four fundamental rules, the same test must obviously not be used for different 'shifts' of an exam, in which different students sit down at the same computer, and where the start and finish times that have been set actually relate to the start of the first 'shift' and the end of the last one. It is also assumed that the computer that students are using has not been used previously by other students without having been cleaned of any type of file that can be shared (such as by making a print screen of the answers, or saving the answers on a text file to be used by the person who next sits at that computer).

The system can be used in real-time or as a tool for auditing after the exam has taken place.

In either case, the teachers responsible for the Course Unit will be in possession of an attendance sheet, which provides a complete list containing the photograph, name and ID of the students, which can be printed out and then given to the students to sign. This is the method used to validate the presence of the student in the room and on the computer the IP of which has been attributed to them.

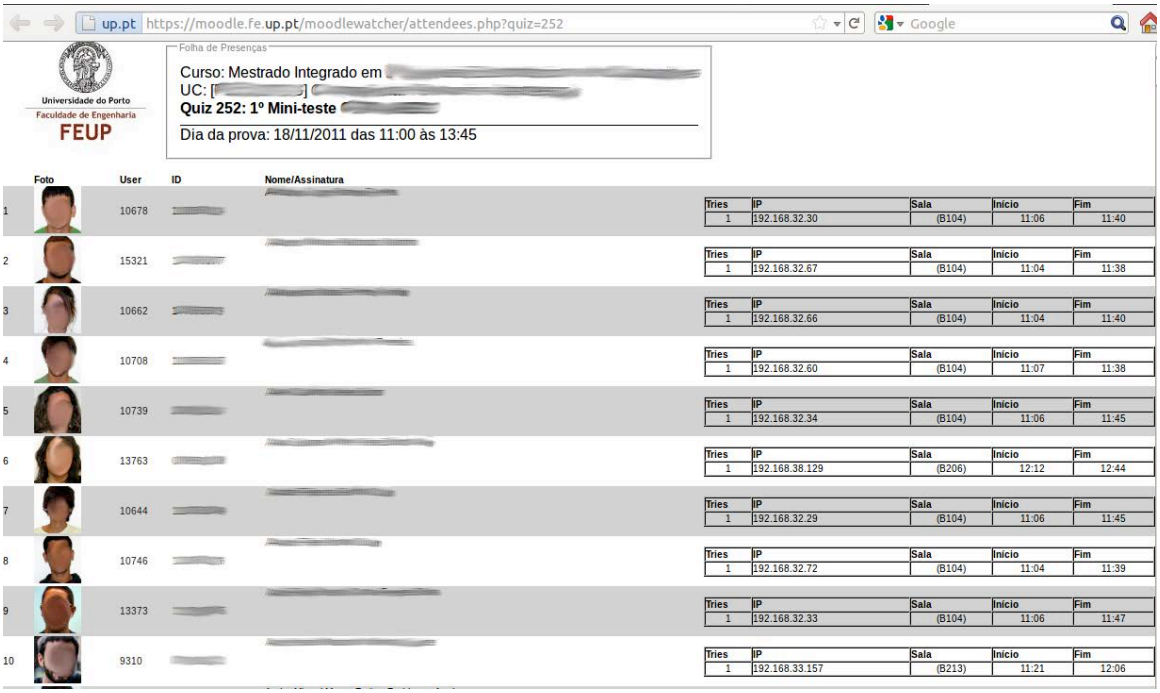

Figure 1: Attendance sheet

Whenever the MoodleWatcher page that relates to the quiz in question is refreshed, the system immediately recalculates all the information available and shows an "ATTENTION!" or "Warning!" message in relation to the cases that have been identified as being suspect, classified by degree of severity.

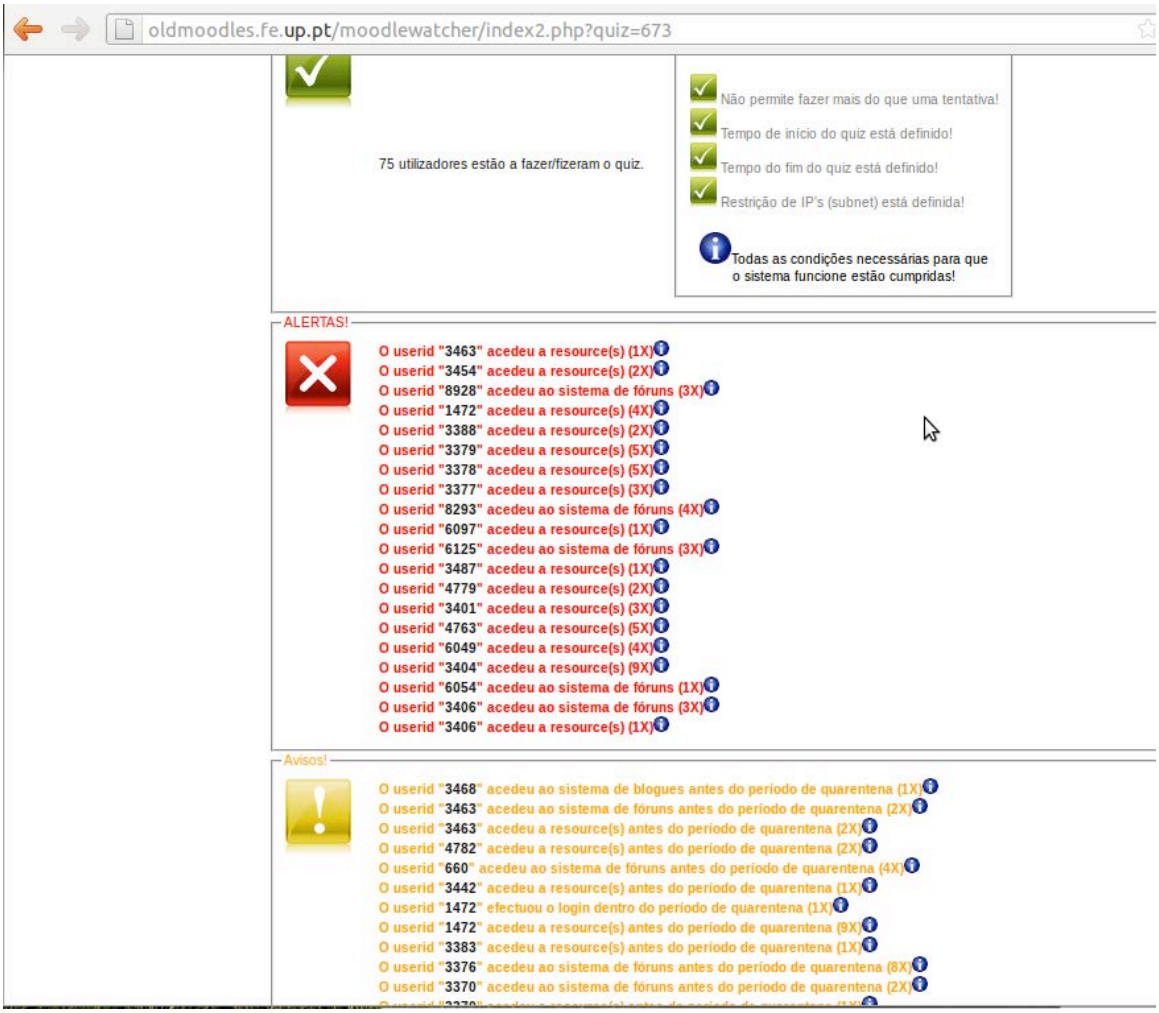

Figure 2: Dashboard view

With "Warning!" messages, less severe cases would include situations such as:

- 'User ID X has logged in BEFORE the start of the quiz!' which indicates that the student has accessed the room in which the test is to be held before the security perimeter has been set up, allowing them to access (and save on the computer) all kinds of information.
- Other types of warning include "access to the forum/blog/resource/etc. systems BEFORE the quarantine period". The quarantine period is the period of time set out within the definitions of the test, in which a student must not under any circumstances access any type of information except for the test itself. If, immediately before starting the test, a student accesses this type of information, this means that they will potentially have this information available to them during the time that they are taking the test.

All anomalous situations that are detected during the quarantine period will result in the issue of an "ATTENTION!" message. A typical example would be an entry of the type:

- 'User ID "X" has accessed the forum system (3X)', in which the "3X" indicates the number of times that the situation has been detected.

MoodleWatcher may also be used as a tool for the monitoring and auditing of Moodle tests in order to ensure their integrity, allowing a teacher to analyze the path followed by the student. This path is presented in order of time, so as to better highlight any doubts or false positives. At this stage it is best to point out that there may be valid reasons for the above-mentioned situations, and that it is up to the person in charge of the course to distinguish between real episodes of fraud and cases of 'mistaken identity' by looking at the situations in context.

4 CONCLUSIONS

Moodle is very good when used as a tool for monitoring educational progress. As a tool for evaluation, however, it has very serious security-related issues that may put the integrity of tests and examinations carried out on its platform in doubt, depending on the methodology of evaluation used. Although these situations have not yet been corrected, this new tool offers a much tighter level of control of the exam room. Without intruding on individual privacy, it provides teachers with the knowledge that they need to identify the majority of cases of fraud, perhaps not immediately, but during a later audit which can be carried out as and when required.

The script do_i_need_moodlewatcher.php was made available to the public domain, and can be used by any Moodle administrator that has direct access to the config.php Moodle configuration file. It will quickly check for some popular scams in the Moodle quizzes module, and provide enough information to evaluate the necessity of implementing a full-blown MoodleWatcher assessment.

Once FEUP students realized that MoodleWatcher was in place, we noted a huge decrease in the number of anomalous situations detected.

Nonetheless, in the recent months since the system has been fully functional, there have still been students that have felt the need to test the effectiveness of the system the hard way, despite the warnings that were continually issued.

5 FUTURE PERSPECTIVES

Analysis of logs using data-mining tools in order to find new behavioural patterns is a top priority. Some suggestions for improving Moodle security are also being studied. These include:

a) Implementation of a "profile (role)" of a “Student Taking an Exam (inexam)” (i) and of a “Program/Course Coordinator (pc-coordinator)” (ii). In the case of (i), its use would have to occur automatically whenever a student took a test; or manually, to make it possible for all students who came to take tests in shifts to only be able to access the test itself throughout the total time reserved for the various tests taking place. The justification for the creation of the second profile (ii) is to enable the possibility of having an entity that could carry out transversal audits on a variety of courses at the same time, without the need to have administrator privileges.

b) Blocking access to all unauthorized material during a determined test, using the "inexam" profile in the following way: the exam calendar - which would also have to be created - would change the profiles of all the students from “student” to “inexam” during the period in which the test is taking place. With this profile, only those students registered to take the test would be able to access it, and would only be able to take the test on the defined subnet. Also, only those students who had registered for a test would be allowed to gain access via an IP on that same subnet. On conclusion of the test, the profile would revert to its normal state.

c) Association, for the time period set aside for the test, of the IP of the first login carried out by the student during the exam, and association of the closure of the "quiz attempt" to the “system logout”, at the same time blocking all access to the account by means other than that of the blocked IP. The teacher will obviously need to be able to unblock the user account if necessary, even if only to deal with the technical problems that sometimes crop up (a student's computer malfunctioning, for example).

REFERENCES

[1] Matos, R., 2011, Do I need MoodleWatcher Audit Report? test script, *How to catch/avoid quiz cheating students Community Discussion forum*, http://moodle.org/pluginfile.php/134/mod_forum/attachment/817464/do_i_need_moodlewatcher.php (October, 2011)